UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/989,087	11/21/2001	Anthony V. Bartram	P/63133	9294

7590 08/25/2005

Kirschstein, Ottinger, Israel & Schiffmiller, P.C.
489 Fifth Avenue
New York, NY 10017-6105

EXAMINER	
KHOSHNOODI, NADIA	

ART UNIT	PAPER NUMBER
2133	

DATE MAILED: 08/25/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/989,087	BARTRAM, ANTHONY V.	
	Examiner	Art Unit	
	Nadia Khoshnoodi	2133	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 September 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 November 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *2/9-16-2003*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Specification

The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

The following title is suggested: Communication System using Random Number Sequences for Successive Cipher Generation.

Claim Rejections - 35 USC § 103

I. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

II. Claims 1, 4-5, 9, and 12-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tan, US Patent No. 6,490,353 and further in view of Dent, US Patent No. 5,148,485.

As per claims 1 and 9:

Tan substantially teaches a communication system/method comprising: a communication channel having ends; at one end of said channel: (i) a first cipher generator for generating a succession of ciphers, said generator including a first random number generator for generating a sequence of random numbers, each cipher of said succession of ciphers being based on a respective successive portion of said sequence of random numbers (col. 8, lines 45-51 and col. 9, line 65 – col. 10, line 47); and (ii) a symmetric encryptor for encrypting successive amounts of information for transmission to the other end of said channel, each amount of information being

encrypted using a respective one of said succession of ciphers (col. 10, lines 48-63); and, at the other end of said channel: (i) a second cipher generator for generating the same said succession of ciphers as the first cipher generator, said second cipher generator including a second random number generator for generating the same said sequence of random numbers as said first random number generator (col. 10, line 64 – col. 11, line 4); and (ii) a symmetric decryptor for decrypting the encrypted successive amounts of information received from said one end of said channel, each amount of information being decrypted using the same respective one of said succession of ciphers as was used to encrypt it by said encryptor at said one end of said channel (col. 13, lines 55-64), wherein each of said first and second cipher generators is signaled to cause it to generate the next cipher in said succession of ciphers, the derivation of the signaling being independent of the information being transmitted (col. 18, lines 51-54).

Not explicitly disclosed is the second cipher generator for generating in synchronism with said first cipher generator the same said succession of ciphers as the first cipher generator. However, Dent teaches that the generator should be in synchronism with the key generator to ensure that the message is properly decoded. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Tan for the second cipher generator to generate the same succession of ciphers as the first cipher generator in synchronism. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Dent in col. 11, lines 1-29.

As per claims 4 and 12:

Tan and Dent teach the system/method according to claims 1 and 9. Furthermore, Dent teaches wherein a supply to said symmetric encryptor of each of said successive amounts of information, is signalled to both said first and second cipher generators, whereupon the generators synchronously generate the same next cipher in said succession of ciphers (col. 11, lines 1-29).

As per claims 5 and 13:

Tan and Dent substantially teach the system according to claims 1 and 9. Furthermore, Tan teaches wherein said symmetric encryptor is a block symmetric encryptor and said symmetric decryptor is a block symmetric decryptor (col. 9, lines 49-64).

III. Claims 2-3 and 10-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tan, US Patent No. 6,490,353 and Dent, US Patent No. 5,148,485 as applied to claims 1 and 9 above, and further in view of Schneier, *Applied Cryptography*.

As per claims 2 and 10:

Tan and Dent substantially teach the system/method according to claims 1 and 9. Furthermore, Tan teaches the system/method further comprising: at said one end of said channel: (i) means for generating a seed sequence of random numbers, which seed sequence is used by said first random number generator to generate said sequence of random numbers (col. 8, line 38 – col. 9, line 48).

Not explicitly disclosed is (ii) an asymmetric encryptor for encrypting said seed sequence for transmission over said channel to said other end of the channel; and, at said other end of said channel: (i) an asymmetric decryptor for decrypting the encrypted seed sequence received from said one end of the channel, said second random number generator using the decrypted seed

sequence to generate said same sequence of random numbers as said first random number generator. However, Schneier teaches that using public key cryptography for encrypting a key that was derived from a symmetric algorithm is a good way to keep the key secure and also not suffer from the slow computational key. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Tan to use public key encryption for encrypting the seed which is used in order to generate the same sequence of random numbers at the other end of the channel. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Schneier on page 33.

As per claims 3 and 11:

Tan, Dent, and Schneier substantially teach the system according to claim 2. Furthermore, Schneier teaches wherein said asymmetric encryptor and said asymmetric decryptor employ public key cryptography (page 33).

IV. Claims 6-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tan, US Patent No. 6,490,353 and Dent, US Patent No. 5,148,485 as applied to claim 1 above, and further in view of Ehrat, US Patent No. 3,678,198.

As per claim 6:

Tan and Dent substantially teach the system according to claim 1. Furthermore, Tan teaches wherein said first and second cipher generators include: first means for receiving said sequence of random numbers (col. 9, line 65 – col. 10, line 16); a plurality of subsidiary cipher generators (col. 7, line 66 – col. 8, line 25), said first means switching said successive portions of said sequence of random numbers between said plurality of subsidiary cipher generators, each

cipher generated by a subsidiary cipher generator being based on a respective said random number sequence portion switched to it by said first means (col. 10, lines 37-47); and second means for switching in turn between said subsidiary cipher generators to provide said succession of ciphers (col. 13, lines 60-64).

Not explicitly disclosed are first switching means and second switching means for carrying out the switching operations. However, Ehrat teaches different switching states. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Tan to specifically use switching means depending on the cipher generator chosen at random. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Ehrat in col. 3, lines 9-62).

As per claim 7:

Tan, Dent, and Ehrat substantially teach the system according to claim 6. Furthermore, Ehrat teaches wherein said plurality of subsidiary cipher generators is two subsidiary cipher generators, and said first and second switching means switch simultaneously but to different ones of said two subsidiary cipher generators (col. 3, line 64 – col. 4, line 25).

As per claim 8:

Tan, Dent, and Ehrat substantially teach the system according to claim 6. Furthermore, Dent teaches wherein each said subsidiary cipher generator comprises: third switching means; a plurality of exclusive OR (XOR) gates (, said third switching means switching random numbers received by the subsidiary cipher generator between said plurality of XOR gates; and a plurality of registers, one in respect of each XOR gate, each register both receiving the output of, and

providing a further input to, its respective XOR gate, the contents of said plurality of registers constituting the cipher generated by the subsidiary cipher generator (col. 14, line 21 – col. 15, line 59).

V. Claims 14-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tan, US Patent No. 6,490,353 and further in view of Ehrat, US Patent No. 3,678,198.

As per claim 14:

Tan substantially teaches a cipher generator for generating a succession of ciphers, said generator comprising: a random number generator for generating a sequence of random numbers (col. 8, lines 45-51 and col. 9, line 65 – col. 10, line 47); first means for receiving said sequence of random numbers (col. 9, line 65 – col. 10, line 16); a plurality of subsidiary cipher generators (col. 7, line 66 – col. 8, line 25), said first means switching said successive portions of said sequence of random numbers between said plurality of subsidiary cipher generators, each cipher generated by a subsidiary cipher generator being based on a respective said random number sequence portion switched to it by said first means (col. 10, lines 37-47); and second means for switching in turn between said subsidiary cipher generators to provide said succession of ciphers (col. 13, lines 60-64).

Not explicitly disclosed are first switching means and second switching means for carrying out the switching operations. However, Ehrat teaches different switching states. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Tan to specifically use switching means depending on the cipher generator chosen at random. This modification would have been obvious because a

person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Ehrat in col. 3, lines 9-62).

As per claim 15:

Tan and Ehrat substantially teach the generator according to claim 14. Furthermore, Ehrat teaches wherein said plurality of subsidiary cipher generators is two subsidiary cipher generators, and said first and second switching means switch simultaneously but to different ones of said two subsidiary cipher generators (col. 3, line 64 – col. 4, line 25).

VI. Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tan, US Patent No. 6,490,353 and Ehrat, US Patent No. 3,678,198 as applied to claim 14 above, and further in view of Dent, US Patent No. 5,148,485.

As per claim 16:

Tan and Ehrat substantially teach the generator according to claim 14. Not explicitly disclosed is wherein each said subsidiary cipher generator comprises: third switching means; a plurality of exclusive OR (XOR) gates, said third switching means switching random numbers received by the subsidiary cipher generator between said plurality of XOR gates; and a plurality of registers, one in respect of each XOR gate, each register both receiving the output of, and providing a further input to, its respective XOR gate, the contents of said plurality of registers constituting the cipher generated by the subsidiary cipher generator. However, Dent teaches using a plurality of XOR gates, switching data between those gates, as well as a plurality of registers receiving the outputs. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Tan to have a third switching means for switching the random numbers received by the subsidiary cipher generator between

the plurality of XOR gates where there are a plurality of registers constituting the cipher generated by the subsidiary cipher generator. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since it is suggested by Dent in col. 14, line 21 – col. 15, line 59.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady can be reached on (571) 272-3819. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

JOSEPH TORRES
PRIMARY EXAMINER

Nadia Khoshnoodi
Examiner
Art Unit 2133
8/17/2005